REMARKS

Claims 1-27, 41-59, 71 and 72 are pending in this application. After claim amendments herein, claims 1-27, 41-59, 71 and 72 will remain pending in this application.

In the July 13, 2005 Office Action, the Examiner objected to claims 42-48 because they are dependent upon canceled independent claim 41. The Examiner assumed that independent claim 41 was inadvertently canceled by Applicants instead of non-elected claim 40, and in order to expedite complete examination of the application the Examiner examined claim 41 as if it were pending and considered dependent claim 40 as having been canceled from the application. The Examiner is correct -- in the Response to Office Action filed April 25, 2005, Applicants incorrectly showed claim 40 as being pending in the application and claim 41 as having been canceled. Applicants thank the Examiner for detecting this error and for properly considering claim 40 as being canceled and claim 41 as being pending. Applicants have corrected this error in the "Claims" section of this response.

In the July 13, 2005 Office Action, the Examiner rejected claims 1-3, 6, 9, 10, 12-15, 17, 18, 21-26, 49, 50, 53-59, 71 and 72 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent Application Publication No. 2003/0196098 (Dickinson). Applicants traverse this rejection.

Dickinson relates to an e-mail firewall that applies policies to e-mail messages between a first site and a plurality of second sites in accordance with a plurality of administrator selectable policies. The firewall comprises a simple mail transfer protocol (SMTP) relay for causing the e-mail messages to be transmitted between the first site and selected ones of the second sites, and a plurality of policy managers enforce-administrator selectable policies. The policies, such as encryption and decryption policies, comprise at least a first source/destination policy, at least a first content policy and at least a first virus policy, and are characterized by a plurality of administrator selectable criteria, a plurality of administrator selectable exceptions to the criteria and a plurality of administrator selectable actions associated with the criteria and exceptions. The policy managers comprise an access manager, a content manager and a virus manager for restricting transmission of e-mail messages between the first site and the second sites in

accordance with the source/destination policy, the content policy and the virus policy, respectively.

Applicants first point out to the Examiner that independent claims 1, 18, 49, 71 and 72 cannot all be grouped and rejected together because they contain different limitations that make them somewhat different embodiments. The basic difference between these two embodiments is that, in amended claims 1 and 71, the steps of creating a privileged distribution list of intended recipients, restricting access to (and restricting routing of) the privileged digital communication to the intended recipients, and storing the privileged digital communication in a segregated location for privileged digital communications on a data storage device are all taken by a program stored within a memory and executable by a processor, whereas, in claims 18, 49 and 72, the steps of restricting access to and restricting routing of the privileged communication to the intended recipients are taken by an executable module that is attached to the digital communication by a program stored within a memory and executable by a processor.

Dickinson does not anticipate all the elements of these claims. For example, the Examiner states that the limitation "attach a privileged attribute to a digital communication" is taught in Dickinson at paragraphs [0030-0031], where a policy module can be set or attached to an e-mail to require either encryption and/or signature to enforce attorney-client privilege. These paragraphs do not teach what the Examiner states they do.

In the paragraphs immediately preceding paragraphs [0030-0031], Dickinson discusses the manner in which messages received from internal and external sites are processed by a policy engine, which is implemented as a program executed by a digital computer, and a plurality of policy managers, which comprise a plurality of modules for enforcing policies directed to specific aspects of e-mail messages, such as source/destination access policies, content control policies, virus control policies and security (encryption/decryption) policies, that have been selected by the e-mail firewall administrator. The policy engine, using the policy managers to enforce the pre-selected policies, determines which policies are applicable to a message by building a list of policies for the sender (source) of the message and building a list policies for each recipient. The policy engine calls the policy managers to apply each policy, based upon

their order of priority, and then receives results from policy managers and transmits messages to the SMTP relay module in accordance with the received results. The results received by the policy engine comprise actions such as disposition, annotation, and notification, and the result of processing of a message by the policy engine can result in generation of a plurality of additional messages, for example, for notification to the sender or recipient, or to the system administrator.

Paragraphs [0030-0031] refer to one embodiment wherein security usage policies specify that certain users, under certain conditions, should perform encryption and/or signature at the desktop. The example used in paragraph [0030] is an e-mail from a company's CEO to the company's legal counsel that can be specified to require either encryption and/or signature in order to enforce attorney-client privilege and to preserve encryption policies. Moreover, client security usage policies can be used to specify that messages, which are already in encrypted form and perhaps meet some other criteria, should be preserved and not be processed, modified or encrypted by the e-mail firewall. Paragraph [0031] specifies that policies are entered preferably by an authorized administrator by way of a configuration module in the form of a program executing on a stored program computer and can be applied to users, either individually or by e-mail domains or other groupings.

When the Examiner states that the limitation "attach a privileged attribute to a digital communication" is taught in Dickinson at paragraphs [0030-0031], where a policy module can be set or attached to an e-mail to require either encryption and/or signature to enforce attorney-client privilege, this is not accurate with regard to any of claims 1, 18, 49, 71 and 72. Regarding amended claims 1 and 71, which require that an executable program contained with in a memory "attach a privileged attribute to a digital communication", Dickinson in fact does not teach that the program attaches anything, much less a privileged attribute, to the digital communication. Similarly, regarding claims 18 and 72, which require that an executable program contained with in a memory "attach an executable module to a digital communication" to restrict access to and routing of the digital communication only to intended recipients, and claim 49, which requires creation of an executable module for instructing a computer to restrict access to an attached communication and attaching the executable module to the communication, Dickinson in fact

does not teach that the program attaches anything, much less an executable module, to the digital communication.

Instead, Dickinson teaches that an authorized administrator enters policies by way of a configuration module in the form of a program executing on a stored program computer and can be applied to users, either individually or by e-mail domains or other groupings (see paragraph [0031]), and these policies are applied to sent or received e-mails (see paragraphs [0022-0023]). Thus, while the security policy manager may indeed be set to require encryption and/or signature in order to enforce attorney-client privilege, as alleged by the Examiner, this is done based upon certain criteria present in the e-mail itself (see paragraph [0039]). However, the policy module, i.e., the security policy manager, does not attach an attribute to the e-mail, nor does the policy module itself get attached to the e-mail. Thus, Dickinson does not teach or suggest that a privileged attribute is attached to the digital communication, as required by claims 1 and 71, or that an executable module is attached to a digital communication, as required by claims 18, 49 and 72, to require encryption and/or signature to enforce attorney-client privilege. Accordingly, for this reason, the rejection of claims 1-3, 6, 9, 10, 12-15, 17, 18, 21-26, 49, 50, 53-59, 71 and 72 should be withdrawn.

Furthermore, with regard to claims 1, 18, 49, 71 and 72, the Examiner stated that the claim limitation "store the privileged digital communication in a segregated location on a data storage device" is taught in Dickinson at paragraphs [0010] and [0040-0041], wherein messages may be stored at specific segregated destinations of queues. However, claims 1 and 71 cannot be anticipated because these paragraphs do not teach the claim limitation (claims 18, 49 and 72 do not contain this limitation).

At paragraph [0010], Dickinson states that actions taken by the e-mail firewall after a message is prevented from being transmitted are changeable, such that the message in question may be returned to the sender, stored for viewing by an administrator or deleted. At paragraphs [0040-0041], Dickinson states that a disposition action determines whether the message should continue to the destination or it should be deferred, quarantined, returned to sender or dropped. Messages received from the disposition step are stored in one of the four queues depending upon

the specified disposition of the message: a quarantine queue where messages are stored for subsequent retrieval and review by a system administrator or other authorized person, a retry queue where messages for which delivery has failed are stored for re-attempted delivery, a dead letter queue where messages that continue to be undeliverable after several retries and cannot be returned to the sender are stored, and a defer queue where messages to be delivered automatically at a later time are stored.

In addition, according to paragraph [0041], a configuration module provides a plurality of actions that may be performed on the messages in these queues: either be viewed by the administrator, returned to the sender, deleted, sent to the specified destination and/or saved. It is clear, therefore, that messages are not stored in one of these four queues and also delivered, but rather that messages in one of the designated queues may either by saved or may be acted upon according to the queue's purpose, or both. However, Dickinson does not disclose or suggest that a message is stored in one of the specified queues. Furthermore, specifically with regard to messages that have been designated as privileged, Dickinson does not disclose or suggest that privileged messages are stored in a segregated location.

By contrast, claims 1 and 71 require that the privileged communication be stored in a segregated location on a data storage device (claims 18, 49 and 72 do not contain this limitation). As discussed above, the disposition queues, although they may be segregated, do not save any messages once their disposition has been complete. Moreover, claims 1 and 71 have been amended herein to specify that the segregated location on a data storage device where the privileged communication is stored is segregated for privileged digital communications. Dickinson discloses no location, including any of the disposition queues, that is segregated for privileged communications. Accordingly, for this additional reason, the rejection of claims 1-3, 6, 9, 10, 12-15, 17, 18, 21-26, 49, 50, 53-59, 71 and 72 should be withdrawn.

In addition, with regard to claim 3, the Examiner stated generally that the claim limitation "a segregated server housing the segregated location on a data storage device" is taught in Dickinson at paragraphs [0034-0038]. However, these paragraphs do not teach this claim limitation. Paragraphs [0034-0038] relate to a virtual private network that is created between

two sites that support the S/MIME protocol for the exchange of secure e-mail messages, wherein secure mail servers function as firewalls and perform many of the security functions, such as encryption/decryption, on behalf of client servers. Nowhere in these paragraphs does Dickinson disclose or suggest a segregated server that houses the segregated location where a message that have been designated as privileged is stored on a data storage device. It is important to note that, although paragraphs [0034-0038] of Dickinson are replete with details and reference numbers to the Figures, the Examiner did not specifically refer to one element or structure within Dickinson that shows a segregated server housing the segregated location on a data storage device where the message that has been designated as privileged is stored.

By contrast, claim 3 requires that a segregated server house the segregated location. Moreover, claim 3 has been amended herein to specify that the segregated location on a data storage device where the privileged communication is stored is segregated for privileged digital communications. Not only does Dickinson not disclose a segregated server that houses the segregated location on a data storage device where the message that has been designated as privileged is stored, but Dickinson does not disclose any location whatsoever that is segregated for privileged communications. Accordingly, the rejection of claim 3 should be withdrawn.

Moreover, the Examiner stated generally that claims 57 and 58 are anticipated because, in paragraphs [0009], [0024] and [0030-0031], Dickinson discloses teaches "configuring access rights to the digital communication when the document is opened and to enforce said access rights by managing access to the digital communication and controlling the manipulation of its contents". However, independent claim 57 and its dependent claim 58 do not contain this limitation, such that the Examiner's citation of paragraphs [0009], [0024] and [0030-0031] from Dickinson is inapposite. Claims 57 and 58 both relate to a method for creating a privileged digital document, comprising the steps of creating an executable module that instructs a computer to maintain confidentiality in communication of the privileged digital document to which the executable module is attached by restricting access to the digital document and managing manipulation of its contents, and attaching the executable module to the document.

As discussed previously regarding claims 18, 49 and 72, which require that an executable module be created and/or attached to a digital communication to restrict access to and routing of the digital communication only to intended recipients, Dickinson in fact does not teach that the program attaches anything, much less an executable module, to the digital communication. Similarly, with respect to claims 57 and 58, Dickinson does not, neither in paragraphs [0009], [0024] and [0030-0031] nor elsewhere in the specification, teach or suggest that an executable module is attached to a digital communication, as required by claims 57 and 58, to maintain confidentiality of the communication by restricting access to the digital document and managing manipulation of its contents. Applicants request that the Examiner provide a proper citation for the limitations of these claims or withdraw the rejection.

The Examiner also rejected claims 9, 21 and 54, which depend from independent claims 1, 18 and 49, (and claim 43, which depends from independent claim 41 as being obvious) on the grounds that Dickinson, at paragraphs [0022-0031] in general disclose the limitation "executing automatically and attaching the privileged attribute to particular communications according to predetermined selection criteria". Applicants first note that the limitation cited by the Examiner appears only in claim 9 but not in claims 21 and 54. Instead, claims 21 and 54 contain the limitation that "the program is configured to execute automatically and attach the executable module to particular communications according to predetermined selection criteria". The difference is that in claim 9, as in independent claim 1, the executable program stored within memory attaches the privileged attribute to the selected communications, whereas in claims 21 and 54, as in independent claims 18 and 49, the executable program stored within memory attaches the executable module to the selected communications.

In any case, as discussed previously with regard to independent claims 1, 18 and 49, Dickinson does not teach that the program attaches anything, including neither a privileged attribute nor an executable module, to the digital communication. Instead, as discussed, Dickinson teaches that an authorized administrator enters policies by way of a configuration module in the form of a program executing on a stored program computer, and these policies are applied to sent or received e-mails, and the policy modules do not attach an attribute to the e-mail, nor do the policy modules themselves get attached to the e-mail. It is important to note

that, although paragraphs [0022-0031] of Dickinson are replete with details and reference numbers to the Figures, the Examiner cited generally to these ten (10) paragraphs rather than specifically refer to one specific disclosure of the program executing automatically and attaching the privileged attribute or the executable module to particular communications according to predetermined selection criteria, as required by claims 9, 21 and 54. Thus, Dickinson does not teach or suggest these limitations in claims 9, 21 and 54, and Applicants request that the Examiner withdrawn the rejection of these claims.

The Examiner further rejected claims 10, 22 and 55 (and claim 44 as being obvious) on the grounds that Dickinson discloses "a confidentiality notice that is displayed to a user and acknowledged by the user before displaying the privileged communication" (Applicants note that they have herein amended this claim to more properly claim a method step). However, paragraph [0039] cited by the Examiner with regard to notification actions does not teach this claim limitation. Instead, paragraph [0039] discusses that notification actions cause the sending of one or more e-mail notifications to the sender, recipient, administrator or any e-mail address that is defined by the administrator, when a given policy is triggered. Dickinson further states that notification actions allow specification of whether the original message should accompany the notification, and that disposition action determines whether the message should continue to the destination specified or whether the message should be deferred, quarantined, returned to sender or dropped.

Applicants contend that the discussion in Dickinson regarding notification actions does not teach the claim limitation of displaying a confidentiality notice to a user and requiring that the confidentiality notice be acknowledged by the user before the privileged communication is displayed. Nowhere in the discussion of notification actions does Dickinson teach acknowledgement of privilege prior to display of the privileged communication. While Dickinson mentions that an e-mail notifications may be sent to the recipient prior to delivery of the message, this is not a specific disclosure of the claim limitation that is required in order for the Examiner to make a prima facie case of anticipation of the claim. Accordingly, in the absence of a more specific disclosure of the limitation of claims 10, 22 and 55, Applicants request that the Examiner withdraw his rejection of these claims.

In addition, the Examiner rejected claims 4, 5, 7, 8, 11, 16, 19, 20, 27, 41-48, 51 and 52 under 35 U.S.C. § 103 as obvious over Dickinson.

Regarding independent claim 41, the Examiner states that Dickinson discloses all the elements of this claim except forwarding the communication. However, Applicants contend that, as discussed above with respect to amended claims 1 and 71, Dickinson does not teach that the communication is marked with a privileged attribute or that the communication be stored in a segregated location for privileged data communications on a data storage device, as require din amended claim 41. Dickinson does not teach that the communication is necessarily marked with any attribute but rather that the policy managers enforce their policies based upon e-mail criteria. In addition, Dickinson discloses no location, including any of the disposition queues, that is segregated for storage of privileged communications. Therefore, Applicants respectfully request that the Examiner withdraw his obviousness rejection of claim 41.

With regard to all other claims 4, 5, 7, 8, 11, 16, 19, 20, 27, 42-48, 51 and 52 rejected under 35 U.S.C. § 103 as obvious over Dickinson, Applicants respectfully submit that these claims should be allowable based upon their dependencies upon base claims that are allowable, as discussed above, and that the rejections of these claims should be withdrawn.

Conclusion

Reconsideration of the present application, as amended, is requested. If, upon review, the Examiner is unable to issue an immediate Notice of Allowance, the Examiner is respectfully requested to telephone Applicant's undersigned attorney in order to resolve any outstanding issues and advance the prosecution of the case.

An early and favorable action on the merits is earnestly solicited.

Respectfully submitted,
DAVIDSON, DAVIDSON & KAPPEL, LLC

By: _____
Morey B. Wildes
Reg. No. 36,968

Davidson, Davidson & Kappel, LLC
485 Seventh Avenue, 14th Floor
New York, NY 10018
(212) 736-1940